REMARKS

Posture of the case

Claims 1-23 were originally filed on December 12, 2004. A first, nonfinal Office action of April 3, 2007, rejected all claims under 35 U.S.C. 103(a). In order to overcome the rejections, Applicant responsively canceled claims 1-23 and submitted new claims 24-44.

The present, final Office action of October 17, 2007 rejects all claims.

Claim Rejections - 35 USC § 112

Claims 24-44 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the final Office action asserts that because claims 24, 31, and 38 recite "detecting whether the as least one changed replica is greater in number than a predetermined number" it is unclear how to compare the changed replica with a predetermined number. Applicant has responsively amended claims 24, 31, and 38 to overcome the rejection. No new matter is added, since the original application provides support. Regarding claims 24, 31, and 38, see original published application, regarding the claimed "nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first has value," see paragraph 0045 (i.e., "If the file has been modified, a hash value computed after the change will differ from a hash value computed before the change . . .") and regarding the claimed "detecting that a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one," see paragraph 0097 (detecting a vulnerability exists responsive to the hash value comparison indicating more than one changed replica of the resource, i.e., more than a predetermined number, where the predetermined number is at least one.)

Claim Rejections - 35 USC § 102

Claims 24-29, 31 -36, and 38-43 stand rejected under 35 U.S.C. 102(e) as being anticipated by Radatti (US 7,143,113).

Applicant has responsively amended claims 24, 31, and 38 to more particularly point out that action is taken only if more than one changed replica is detected. Applicant respectfully submits that amended, independent claims 24, 31, and 38 are patentably distinct.

The present application, as published, paragraph 0097, teaches the following:

> A further embodiment of the invention uses statistical observation of the pattern of creation of new hashes to identify sudden changes within a network. For example, if newly computed hash values are compared with stored hash values and a large number of copies of a specific hash value MD.sub.1 can be seen to have changed, this implies that the corresponding copies of the resource represented by hash value MD.sub.1 have also changed. This could mean that a group of users are upgrading from one file version to another (for example if MD.sub.1 consistently changes to MD.sub.2) or that a virus is spreading through the system. The latter is most likely if a large number of copies of MD.sub.1 have remained unchanged for a long period and are then suddenly replaced by a large number of different hash values--indicating the probable spread of a polymorphic virus. The comparison of hash values can be used once again to determine which resources require a virus scan and which do not.

In this described embodiment of the present invention, more than one file must be changed in order to indicate a vulnerability.

Amended, independent claims 24, 31, and 38 indicate first hash values, derived from and representing a plurality of replicas of a resource, are computed and stored. Current hash values for the replicas of the resource are computed. Further, independent claims 24, 31, and 38 go on to state that the current and first hash values are compared "in order to identify whether all the hash values match." Still further, independent claims 24, 31, and 38 recite "detecting that a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one." The cited references do not teach or suggest this combination of features.

In particular, the cited reference, Radatti, actually teaches away from amended independent claims 24, 31, and 38 in at least one respect. That is, Radatti teaches that *any* difference in hash value comparison indicates a vulnerability, whereas amended independent claims 24, 31, and 38 make it clear that according to the claimed arrangement in the present

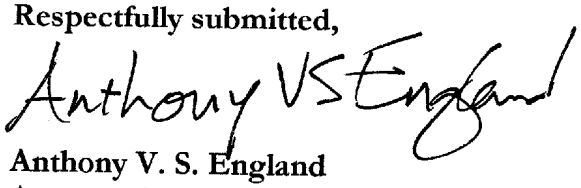
application, a vulnerability is indicated only if there is *more than one* changed replica (as indicated by differences in first and current hash values of the respective replicas). For example, Radatti, col. 7, lines 47-58, teaches that the system responds to even a single change in a file, by stating that ". . . *any* variation from the secure system state will be detected. The nature of the file will not matter insofar as *any file* that modifies the system and/or its files will be detected" (emphasis added). This is different than detecting a vulnerability responsive only to a plurality of changes in a replica (e.g., a file), i.e., a "detecting that a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one," as claimed in the present case.

The claimed arrangement in which a vulnerability is not indicated for only a single changed replica (e.g., file) is not taught or suggested by the cited art. For at least this reason, independent claims 24, 31, and 38 are patentably distinct. In addition, dependent claims 25-30, 32-37, and 39-44 are allowable at least because they depend on allowable dependent claims.

REQUESTED ACTION

For the reasons explained herein above, Applicant contends that the claims as amended herein are patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,



Anthony V. S. England
Attorney for IBM Corporation
Registration No. 35,129
512-477-7165
a@aengland.com